Steve W. Berman (*pro hac vice* pending)
Thomas E. Loeser (SBN 202724)
HAGENS BERMAN SOBOL SHAPIRO LLP
1918 Eighth Avenue, Suite 3300
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
steve@hbsslaw.com
toml@hbsslaw.com

Mark P. Robinson, Jr. (SBN 054426)
Daniel S. Robinson (SBN 244245)
Wesley K. Polischuk (SBN 254121)
ROBINSON CALCAGNIE ROBINSON SHAPIRO DAVIS, INC.
19 Corporate Plaza Drive
Newport Beach, California 92660
Telephone: (949) 720-1288
Facsimile: (949) 720-1292
mrobinson@rcrsd.com
drobinson@rcrsd.com
wpolischuk@rcrsd.com

Attorneys for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FAZI ZAND, individually and on behalf of all others similarly situated, Plaintiff, v. ANTHEM, INC., d/b/a Anthem Health, Inc., an Indiana Corporation, THE ANTHEM COMPANIES, INC., an Indiana Corporation Defendants.	Case No. CLASS ACTION COMPLAINT **DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

Page(s)

1. A national health insurer with computer systems that store highly sensitive customer information including Social Security Numbers (SSNs) along with name, address, date of birth, and financial information must ensure that its customers' and employee's personal and financial information is safeguarded from theft. When a data breach affecting up to 80 million records of past and present customers and employees occurs, a national health insurer must *immediately and accurately* notify its customers and employees to prevent such customers and employees from becoming victims of identity theft. This lawsuit stems from Anthem's failure to follow these two simple rules.

I. FACTS

2. Anthem is the parent company of Anthem Blue Cross and Blue Shield, and the second largest health insurer in the United States. Anthem resulted from the 2004 merger of Anthem and WellPoint. In its Fourth Quarter 2014 results, Anthem stated it had approximately 37.5 million health care enrollees. It claimed 2014 net income totaling approximately $2.6 billion.

A. The Anthem Data Breach

3. On February 4, 2015, Anthem first disclosed that its computer systems had been hacked. The company stated it is continuing its investigation into the scope of the breach, but indicated that between approximately December 10, 2014 and January 27, 2015 unknown hackers were able to breach a database that contained as many as 80 million records of current and former customers, as well as employees (the "Anthem data breach").[1]

4. However, even this first disclosure has already been challenged by experts. Brian Krebs, the noted cyber-security journalist who first broke the story on the Target data breach has reported that the Anthem data breach may have started as early as April 2014.[2]

5. The information accessed included names, addresses, birthdates, email, and employment information, income data, Member ID/Social Security numbers.[3]

---

[1] *See* Millions of Anthem Customers targeted in Cyberattack, NEW YORK TIMES, Reed Ableson and Matthew Goldstein, Feb. 5, 2015.

[2] http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/.

[3] *See id.*

6. The massive Anthem data breach could have been prevented and should have been detected and disclosed earlier. Anthem claims it was first detected on January 27, 2015, but not disclosed for a week. Health care companies, including Anthem, were specifically warned by the FBI in 2014 of the increasing threat to health care companies from hackers. Yet, on information and belief, Anthem did not take the necessary and reasonable steps to protect its data storage systems from attack.

7. Reports on the Anthem data breach indicate that administrative access to the complete customer records database was available with a simple "one-factor" authentication. Meaning that by obtaining just a log-in and password, hackers obtained unfettered access.

8. Anthem has indicated that as many as five employee log-ins and passwords were compromised. But that access could have been thwarted entirely if Anthem had used a "two-factor" authentication process—that is a process which required a personal device (such as a 'dongle' or electronic keycard) in addition to a log-in and password for access. "[Two-factor authentication] is considered best practice for any type of company with sensitive data, and it's rather revealing of the security health of the healthcare industry if the second-largest health insurer didn't have it in place."[4]

9. Anthem has a long history of failure to adequately protect consumer data and has been hacked on multiple occasions. For example, in 2010, a security breach allowed public access to medical records of 616,000 customers.[5] As described in the civil action Settlement Agreement entered on April 18, 2011, Anthem, then called WellPoint, learned as follows:

> In February 2010, an individual who had submitted an application to WellPoint for health benefits coverage on behalf of her minor dependent informed the company that she believed Internet users could access the application that she had submitted as well as other applicants' confidential information on the

[4] https://www.duosecurity.com/blog/four-years-later-anthem-breached-again-hackers-stole-employee-credentials.

[5] *See* http://www.healthsecuritysolutions.com/2013/07/wellpoint-website-vulnerability-leads-to-1-7-m/#.VNQKUE10yUk (Anthem was then called Wellpoint) (last accessed Feb. 6, 2015).

> WellPoint web servers by deleting characters at the end of the web address for WellPoint's customer interface website.[6]

As a part of the Settlement Agreement, Anthem acknowledged that:

> [T]he username, password and encryption security protections were not transferred to the upgraded web servers and, as a result, the electronically stored personal identifying information and personal health information of WellPoint customers, enrollees or subscribers was unprotected by username, password and encryption from on or around October 23, 2009 through on or around March 10, 2010 . . . .[7]

10. Anthem, as Wellpoint, also paid a $1.7 million penalty to the Department of Health and Human Services (HHS) as part of that breach.[8]

11. In that settlement:

> The Resolution Agreement reached between Wellpoint, Inc. and HHS OCR stated several findings from the HHS investigation following the HIPAA violation. According to the report, Wellpoint, Inc. failed to implement appropriate security procedures and policies prior to allowing access to ePHI, therefore violating HIPAA security policies. The company also failed to perform technical evaluations of system security following software upgrade and failed to utilize adequate technology to identify users seeking access to sensitive information. These findings indicated inadequacies in the Wellpoint, Inc. system and clear violations of HIPAA regulations, but were not an admission of liability by the company. The Resolution Agreement ultimately determined the penalty due to HHS OCR for HIPAA violations, but did not include monies payable to individual clients who filed lawsuits following data compromise.[9]

12. In 2007, Wellpoint lost names, SSNs and other data regarding 196,000 customers.[10]

13. As reported on CBS Money Watch, "Not all data breaches are created equal, and the Anthem health insurance hack is about as bad as they get for consumers."[11] This data breach is far

---

[6] The full text of the Settlement Agreement in *Blue Cross of California Website Security Cases* (California Superior Court JCCP 4647) can be found at https://anthembluecrosssecuritysettlement.com/SettlementAgreement.pdf (last accessed Feb. 6, 2015).

[7] *See id.*

[8] *See id.*

[9] *Id.*

[10] http://www.itsecurity.com/features/top-security-breaches-2007-012208/ (last accessed Feb. 6, 2015).

more serious than recent retail chain data breaches where credit card information was stolen, such as at the retail chain, Target. "On its website, [Anthem] highlights the fact that no credit or debit card information was stolen, knowing full well that's the least dangerous information to lose," said Neal O'Farrell, a security and identity theft expert for CreditSesame.com. "The victims of this breach, who lost their name, date of birth, and Social Security number to hackers, now face a lifetime of potential victimization."[12]

14. There is little doubt victims of the Anthem data breach will suffer significant and persistent financial harm as a result. "This time the crooks got Social Security numbers. For identity thieves, the Social Security number is the key that unlocks the vault, and they now have millions of them."[13]

15. As noted in another Moneywatch article, "When a thief gets that information, we call that the perfect identity," said John Dancu, the chief executive of technology security company IDology. "Financial institutions have been hit for several years so they have gone in and tried to harden their systems, and the next place for the fraudsters to hit is the medical system."[14]

16. In addition to selling Anthem customer data to other fraudsters on the black market, the thieves could use the data to set up fraudulent financial accounts in victims' names, such as credit card accounts, Dancu noted.[15]

17. With access to Social Security numbers, birthdates, employment information and income data, fraudsters could also file false tax returns, with the goal of claiming a fraudulent

---

[11] Mitch Lipka, Anthem Data Breach: Steps you need to take, available on 2/5/15 at http://www.cbsnews.com/news/what-you-need-to-know-about-the-anthem-hack/ (last accessed Feb. 6, 2015).

[12] *Id.*

[13] *Id.*

[14] http://www.cbsnews.com/news/how-hackers-might-use-your-stolen-anthem-data/ (last accessed Feb. 6, 2015).

[15] *Id.*

refund. That's a growing problem in the U.S., with the Internal Revenue Service investigating almost 1,500 cases in 2013, a jump or 66 percent from the previous year.[16]

18. Alarmingly, Anthem has not notified the particular victims of the data breach, and says that process could take weeks. All the while, thieves have everything they need to open false credit card accounts, bank accounts, loans, and can even file false tax returns and steal refunds owed to Anthem customers and employees whose records have been stolen.

19. As reported in Business Day, "This is one of the worst breaches I have ever seen," said Paul Stephens, director of policy and advocacy for the Privacy Rights Clearinghouse, a nonprofit consumer education and advocacy group. "These people knew what they were doing and recognized there was a treasure trove here, and I think they are going to use it to engage in very sophisticated kinds of identity theft."[17]

B. Anthem Collects its Customers' and Employees Personal Information

20. Anthem is one of the three largest health insurance systems in the United States and is currently ranked 38th on the "Fortune 500" list of top US companies.[18] Anthem markets and sells health insurance directly to millions of consumers through its websites and the Blue Cross/Blue Shield "brands."

21. Anthem is acutely aware that the customer and employee information it stores is highly sensitive and highly valuable to identity thieves and other criminals. On its website, Anthem describes its data security policies.[19]

22. Anthem states:

> **Personal Information (Including Social Security Number) Privacy Protection Policy**
>
> Anthem Blue Cross and Blue Shield maintains policies that protect the confidentiality of personal information, including Social Security numbers,

[16] *See id.*

[17] http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html (last accessed Feb. 6, 2015).

[18] http://fortune.com/fortune500/ (Anthem is listed under its prior name, Wellpoint) (last accessed Feb. 6, 2015).

[19] *See* https://www.anthem.com/health-insurance/about-us/privacy (last accessed Feb. 6, 2015).

obtained from its members and associates in the course of its regular business functions. Anthem Blue Cross and Blue Shield is committed to protecting information about its customers and associates, especially the confidential nature of their personal information (PI).

Personal Information is information that is capable of being associated with an individual through one or more identifiers including but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number, and does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

• Anthem Blue Cross and Blue Shield is committed to protecting the confidentiality of Social Security numbers and other Personal Information.

• Anthem Blue Cross and Blue Shield's Privacy Policy imposes a number of standards to:

- guard the confidentiality of Social Security numbers and other personal information,
- prohibit the unlawful disclosure of Social Security numbers, and
- limit access to Social Security numbers.

Anthem Blue Cross and Blue Shield will not use or share Social Security numbers or personal information with anyone outside the company except when permitted or required by federal and state law.

Anthem Blue Cross and Blue Shield Associates must only access Social Security numbers or personal information as required by their job duties. Anthem Blue Cross and Blue Shield has in place a minimum necessary policy which states that associates may only access, use or disclose Social Security numbers or personal information to complete a specific task and as allowed by law.

Anthem Blue Cross and Blue Shield safeguards Social Security numbers and other personal information by having physical, technical, and administrative safeguards in place.

23. There is little question that the above policy demonstrates Anthem was well aware of the need for it to protect consumers highly valuable "PI", including SSNs.

24. While Anthem's collection of customer and associate data may itself be legal, it cannot be questioned that by collecting and storing such extensive and detailed customer data, Anthem creates an obligation for itself to use every means available to it to protect this data from falling into the hands of criminals.

25. The most rudimentary of the steps Anthem could have and should have taken is encryption. That is, Anthem should have converted customers' and employees' sensitive information into coded strings that would not be immediately useful, or even identifiable to cyber-thieves. Yet Anthem did not even take that step. It stored its customers and employees most sensitive information, including SSNs, and income information in plain text, readily identifiable and usable by anyone.[20]

26. Anthem did not control access to PHI (Protected Health Information) and PII (Personally Identifiable Information) in a manner consistent with healthcare industry standards for the protection of sensitive information or with health industry regulations defined by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA Security Rule mandates that all PHI is protected, that an unauthorized disclosure of PHI is treated as a security incident (HIPAA Security Rule, 45 C.F.R. § 164.304) and that security incidents are met with a security incident response. HIPAA Security Rule, 45 C.F.R. § 164.308(a)(6). The HIPAA security rule refers to several standard, guideline, or recommendation documents released by the National Institutes of Standards and Technology as methods to achieve components of HIPAA compliance. Federal Register Vol. 68, No. 34, pp. 8346, 8350, 8352, and 8355.

C. The Data Breach Harmed Plaintiff and Other Class Members

27. As a result of Anthem's unfair, inadequate, and unreasonable data security, cyber-criminals now possess the personal and financial information of Plaintiff and the Class. Unlike the credit card data breaches, like those recently at Target Corp. and Home Depot, the harm here cannot be attenuated by cancelling and reissuing credit cards. With SSN's, names, addresses, emails, and employment and income information, criminals can open entirely new credit accounts and bank accounts, and garner millions through fraud that victims will not be able to detect until it is too late. Victims' credit profiles can be destroyed and they will lose the ability to legitimately borrow money, obtain credit, or even open bank accounts. Further, criminals can file false federal and state tax returns in their names, preventing or at least delaying victims' receipt of their

[20] *See* http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html (last accessed Feb. 6, 2015).

legitimate tax refunds and potentially making victims targets of IRS and state tax investigations. At the very least, victims must add themselves to credit fraud watch lists, which substantially impair victims' ability to obtain additional credit. Many experts advise a flat out freeze on all credit accounts, making it impossible to rent a car, get student loans, buy or rent furniture or a new TV, let alone complete a major purchase such as a new car or home.

28. Immediate notice of a data breach is essential to obtain the best protection afforded by identity theft protection services. Anthem failed to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiff and the Class resulting from the breach. Anthem knew its systems were compromised at least as early as January 30, 2015, yet it made no disclosures until February 4, 2015. Even then, it stated it would not notify the victims "for several weeks." Such delays are unwarranted, and increase directly the likelihood that thieves will be able to steal victims' identities before victims even know that they are at risk.

29. Personal and financial information is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other personal information on a number of Internet websites. A credit card number trades for under $10 on the black market. Magnetic track data increases the price, and a card with full personal information such as an address, phone number, and email address ("fullz") are traded at around $25 per record.[21]

30. But this breach is far more valuable. The Anthem data breach consists of 80 million records that include name, address, email, SSN, birthdate, employment information and even income. Complete identity records like those at issue here can sell for $250-$400 on the black market, making this a breach potentially worth in excess of $20 billion to cybercriminals.[22]

31. The personal and financial information that Anthem failed to adequately protect, including Plaintiff's identifying information and SSN, is "as good as gold" to identity thieves

[21] http://motherboard.vice.com/blog/its-surprisingly-cheap-to-buy-stolen-bank-details (last accessed Feb. 6, 2015).

[22] *See* http://www.secureworks.com/assets/pdf-store/white-papers/wp-underground-hacking-report.pdf at p.4 (last accessed Feb. 6, 2015).

because identity thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, and file false federal and state tax returns.

32. Although Anthem has suggested it may offer free credit monitoring to some customers, the credit monitoring services do little to prevent wholesale identity theft. Moreover, experts warn that batches of stolen information will not be immediately dumped on the black market. "[O]ne year of credit monitoring may not be enough. Hackers tend to lay low when data breaches are exposed…They often wait until consumers are less likely to be on the lookout for fraudulent activities."[23]

33. This is especially true for SSNs, which unlike credit cards, are not reissued. A cybercriminal, especially one with millions of SSN records, can hold on to stolen information for years until the news of the theft has subsided, then steal a victim's identity, credit, and bank accounts, resulting in thousands of dollars in losses and lost time and productivity. Thus, Plaintiff and the Class must take additional steps to protect their identities.

II. JURISDICTION AND VENUE

34. This Court has diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). At least one Plaintiff and Defendant are citizens of different states. The amount in controversy exceeds $5 million, exclusive of interest and costs, and there are more than 100 putative class members.

35. This Court has personal jurisdiction over Anthem because Anthem is licensed to do business in California, regularly conducts business in California, and has minimum contacts with California.

36. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Anthem regularly conducts business and resides in this district, a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims were committed in this district, Plaintiff resides in this district, and property that is the subject of Plaintiff's claims are in this district.

[23] http://online.wsj.com/news/articles/SB10001424052702304856504579337263720948556 (last accessed Feb. 6, 2015).

III. PARTIES

37. Plaintiff Fazi Zand resides in San Francisco, CA and is a current Anthem health insurance customer under Blue Shield Blue Cross.

38. In the first week of February, 2015, Plaintiff read news reports describing the Anthem data breach and indicating that information concerning current and former Anthem customers had been stolen, in addition to records of Anthem employees.

39. On February 4, 2015, Plaintiff received the following email from Anthem:

> Safeguarding your personal, financial and medical information is one of our top priorities, and because of that, we have state-of-the-art information security systems to protect your data. However, despite our efforts, Anthem Blue Cross was the target of a very sophisticated external cyber attack. These attackers gained unauthorized access to Anthem's IT system and have obtained personal information from our current and former members such as their names, birthdays, medical IDs/social security numbers, street addresses, email addresses and employment information, including income data. Based on what we know now, there is no evidence that credit card or medical information (such as claims, test results or diagnostic codes) were targeted or compromised.
>
> Once the attack was discovered, Anthem immediately made every effort to close the security vulnerability, contacted the FBI and began fully cooperating with their investigation. Anthem has also retained Mandiant, one of the world's leading cybersecurity firms, to evaluate our systems and identify solutions based on the evolving landscape.
>
> Anthem's own associates' personal information – including my own – was accessed during this security breach. We join you in your concern and frustration, and I assure you that we are working around the clock to do everything we can to further secure your data.
>
> Anthem will individually notify current and former members whose information has been accessed. We will provide credit monitoring and identity protection services free of charge so that those who have been affected can have peace of mind. We have created a dedicated website - AnthemFacts.com - where members can access information such as frequent questions and answers. As we learn more, we will continually update this website and share that information with you. We have also established a dedicated toll-free number that both current and former members can call if they have questions related to this incident. That number is: 1-877-263-7995.
>
> I want to personally apologize to each of you for what has happened, as I know you expect us to protect your information. We will continue to do everything in our power to make our systems and security processes better and more secure, and hope that we can earn back your trust and confidence in Anthem.

Sincerely,
Joseph Swedish
President and CEO
Anthem, Inc.

40. Plaintiff visited the Anthem website to try and determine whether his records were affected. He found no information on the website that was helpful to him.

41. Plaintiff has not been contacted again by Anthem since the February 4, 2105 email.

42. Plaintiff is highly concerned that his social security number, as well as his wife's and his son's Social Security numbers have been stolen. Plaintiff has contacted Equifax to place a fraud alert on his entire family's credit files.

43. Plaintiff was harmed in having his personal, health, and financial information associated with his health insurance compromised as a result of the Anthem data breach. Plaintiff provided medical information and financial information to Anthem. Anthem's conclusory statements about the breach and the hacker's infiltration of Anthem's network where records were kept without encryption or two-factor password protection makes it likely additional medical information (beyond the fact Plaintiff was covered by Anthem health insurance) and credit card information, were also unsecure and obtained by the unauthorized parties.

44. Plaintiff would not have given his personal health and financial information to Anthem for his health insurance had Anthem informed him that it lacked adequate computer network and data security to secure his and other Anthem customers' personal, health, and financial information.

45. Plaintiff suffered actual injury from having his financial, health, and personal information compromised and stolen as a result of the Anthem data breach, and was further injured by Anthem's failure to provide timely and accurate notice that his data had been breached.

46. Plaintiff suffered actual injury and damages in purchasing insurance from, and paying money to, Anthem before and during the Anthem data breach that he would not have paid Anthem: (1) had it disclosed that it lacked computer network and data security to adequately

protect his and other customers personal, health, and financial information, or (2) had Anthem provided timely and accurate notice that his data had been breached.

47. Defendant Anthem, Inc., doing business as Anthem Health, Inc. is an Indiana corporation registered with the California Secretary of State to do business in California with its corporate headquarters at 120 Monument Circle, Indianapolis, IN.

48. Defendant The Anthem Companies, Inc. is an Indiana corporation, registered with the California Secretary of State to do business in California with its corporate headquarters in Indianapolis, IN.

49. Through its subsidiary Anthem Insurance Companies, Inc., also an Indiana corporation, Anthem, Inc. provides healthcare benefits through Blue Cross and Blue Shield plans in California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia and Wisconsin. Anthem, Inc., The Anthem Companies, Inc., its subsidiaries, and healthcare plans are collectively referred to as "Anthem" in this Complaint

IV. CLASS ALLEGATIONS

50. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action as a national class action for himself and all members of the following Class of similarly situated individuals and entities:

The Nationwide Class

> All persons in the United States whose personal information was compromised as a result of the data breach first disclosed by Anthem on February 4, 2015.

51. Excluded from the Class are Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant.

52. Plaintiff also seeks to certify the following Subclass of the Nationwide Class (the "California Subclasses"):

The California Subclass

All members of the Class who are residents of California or purchased health insurance from an Anthem company in California.

53. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

54. All members of the proposed Class and subclasses are readily ascertainable. Anthem has access to addresses and other contact information for all members of the Class, which can be used for providing notice to Class members.

55. ***Numerosity***. The Class is so numerous that joinder of all members is unfeasible and not practical. While the precise number of Class members has not been determined at this time, Anthem has admitted that 80 million records were stolen relating to past and current customers and employees, and it has over 37 million current health insurance customers.

56. ***Commonality***. Questions of law and fact common to all Class members exist and predominate over any questions affecting only individual Class members, including, *inter alia*:

a. whether Anthem engaged in the wrongful conduct alleged herein;

b. whether Anthem's conduct was deceptive, unfair, and/or unlawful;

c. whether Anthem owed a duty to Plaintiff and members of the Class to adequately protect their personal, health, and financial information;

d. whether Anthem owed a duty to provide timely and accurate notice of the Anthem data breach to Plaintiff and members of the Class;

e. whether Anthem's conduct was likely to deceive a reasonable person;

f. whether Anthem used reasonable and industry-standard measures to protect Class members' personal information;

g. whether Anthem knew or should have known that its data system was vulnerable to attack;

h. whether Anthem should have maintained information of past subscribers in its database instead of purging and deleting all information of non-current subscribers;

i. whether Anthem's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of millions of consumers' personal, health, and financial data;

j. whether Anthem should have notified the public immediately after it learned of the data breach;

k. whether Anthem violated California Business and Professions Code § 17200, *et. seq.*;

l. whether Plaintiff and Class members are entitled to recover actual damages, statutory damages, and/or punitive damages; and

m. whether Plaintiff and Class members are entitled to restitution, disgorgement, and/or other equitable relief.

57. ***Typicality***. Plaintiff's claims are typical of the claims of the Class. Plaintiff and all Class members were injured through the uniform misconduct described above and assert the same claims for relief.

58. ***Adequacy***. Plaintiff and his counsel will fairly and adequately represent the interests of the Class members. Plaintiff has no interests antagonistic to, or in conflict with, the interests of the Class members. Plaintiff's lawyers are highly experienced in the prosecution of consumer class actions and complex commercial litigation.

59. ***Superiority***. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiff and the Class members. Plaintiff and the Class members have been harmed by Anthem's wrongful actions and/or inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Anthem's wrongful actions and/or inaction.

60. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual

members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

61. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2) because Anthem has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

62. The expense and burden of litigation would substantially impair the ability of Plaintiff and Class members to pursue individual lawsuits to vindicate their rights. Absent a class action, Anthem will retain the benefits of its wrongdoing despite its serious violations of the law.

V. COUNTS

COUNT I

Negligence

(On Behalf of Plaintiff and the Nationwide Class)

63. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs.

64. By accepting Plaintiff's and Class members' non-public personal information, Anthem assumed a duty requiring it to use reasonable and, at the very least, industry-standard care to secure such information against theft and misuse.

65. Anthem breached its duty of care by failing to adequately secure and protect Plaintiff's and the Class members' personal information from theft, collection and misuse by third parties.

66. Anthem further breached its duty of care by failing to promptly, clearly, accurately, and completely inform Plaintiff and the Class that their personal information had been stolen.

67. Anthem further breached its duty of care by failing to purge and delete records related to former Anthem customers. There was no legitimate reason for Anthem to retain the information of former customers and store it on their customer records database.

68. Plaintiff and the Class have suffered injury in fact, including monetary damages, and will continue to be injured and incur damages as a result of Anthem's negligence and misconduct.

69. As a direct and proximate result of Anthem's failure to take reasonable care and use at least industry-standard measures to protect the personal information placed in its care, and failure to purge and delete the information relating to former customers, Plaintiff and members of the Class had their personal information stolen, causing direct and measurable monetary losses, threat of future losses, identity theft and threat of identity theft.

70. As a direct and proximate result of Anthem's negligence and misconduct, Plaintiff and the Class were injured in fact by: identity theft; damage to credit scores and credit reports; time and expense related to: (a) finding fraudulent accounts; (b) monitoring their identity; (c) credit monitoring and identity theft prevention; (d) income tax refund fraud the potential for income tax refund fraud; (e) the general nuisance and annoyance of dealing with all these issues resulting from the Anthem data breach; and (j) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the Anthem data breach, all of which have an ascertainable monetary value to be proven at trial.

COUNT II

Negligence *per se*

(On Behalf of Plaintiff and the Nationwide Class)

71. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs.

72. Pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, Anthem had a duty to keep and protect the personal information of its customers.

73. Anthem violated the Gramm-Leach-Bliley Act by failing to keep and protect Plaintiff's and Class members' personal and financial information, failing to monitor, and/or failing to ensure that Defendant complied with data security standards, industry standards, statutes and/or other regulations to protect such personal and financial information.

74. Anthem's failure to comply with the Gramm-Leach-Bliley Act, and/or other industry standards and regulations, constitutes negligence per se.

75. Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security and Privacy Rules, 42 U.S.C. § 1320d, *et seq.*, Anthem had a duty to keep and protect the personal information of its customers.

76. Anthem violated HIPAA by failing to keep and protect Plaintiff's and Class members' personal and financial information, failing to monitor, and/or failing to ensure that Defendant complied with PCI data security standards, statutes and/or other regulations to protect such personal and financial information.

77. Anthem's failure to comply with HIPAA, and/or other industry standards and regulations, constitutes negligence per se.

COUNT III

Breach of Implied Contract

(On Behalf of Plaintiff and the Nationwide Class)

78. Plaintiff realleges and incorporates by reference the allegations contained in preceding paragraphs.

79. Plaintiff and the Class provided their financial and personal information to Anthem in exchange for Anthem's services. Plaintiff and members of the Class entered into implied contracts with Anthem pursuant to which Anthem agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

80. Each purchase for Anthem's services made by Plaintiff and members of the Class were made pursuant to the mutually agreed upon implied contract with Anthem under which Anthem agreed to safeguard and protect Plaintiff's and Class members' personal and financial information, and to timely and accurately notify them that such information was compromised and breached.

81. Plaintiff and Class members would not have provided and entrusted their financial and personal information to Anthem in order to purchase Anthem services in the absence of the implied contract between them and Anthem.

82. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Anthem.

COUNT IV

Unjust Enrichment

(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

83. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs.

84. Plaintiff and Class members conferred a monetary benefit on Anthem in the form of monies paid for the purchase of services during the period of the Anthem data breach.

85. Anthem appreciates or has knowledge of the benefits conferred directly upon it by Plaintiff and members of the Class.

86. The monies paid for the purchase of services by Plaintiff and members of the Class to Anthem during the period of the Anthem data breach were supposed to be used by Anthem, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and members of the Class.

87. Anthem failed to provide reasonable security, safeguards and protection to the personal and financial information of Plaintiff and Class members and as a result, Plaintiff and Class members overpaid Anthem for the services purchased during the period of the Anthem data breach.

88. Under principles of equity and good conscience, Anthem should not be permitted to retain the money belonging to Plaintiff and members of the Class, because Anthem failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' personal and financial information that they paid for but did not receive.

89. As a result of Anthem's conduct as set forth in this Complaint, Plaintiff and members of the Class suffered damages and losses as stated above, including monies paid for Anthem services that Plaintiff and Class members would not have purchased had Anthem disclosed the material fact that it lacked adequate measures to safeguard customers' information and had Anthem provided timely and accurate notice of the data breach, and including the difference

between the price they paid for Anthem's services as promised and the actual diminished value of its services.

90. Plaintiff and the Class have conferred directly upon Anthem an economic benefit in the nature of monies received and profits resulting from sales and unlawful overcharges to the economic detriment of Plaintiff and the Class.

91. The economic benefit, including the monies paid and the overcharges and profits derived by Anthem and paid by Plaintiff and members of the Class, is a direct and proximate result of Anthem's unlawful practices as set forth in this Complaint.

92. The financial benefits derived by Anthem rightfully belong to Plaintiff and members of the Class.

93. It would be inequitable under established unjust enrichment principles of the states where Anthem conducts business for Anthem to be permitted to retain any of the financial benefits, monies, profits, and overcharges derived from its unlawful conduct as set forth in this Complaint.

94. Anthem should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by Anthem.

95. A constructive trust should be imposed upon all unlawful or inequitable sums received by Anthem traceable to Plaintiff and the Class.

96. Plaintiff and the Class have no adequate remedy at law.

COUNT V

Violation of Indiana Code § 24-5-0.5, *et seq.*

(On Behalf of Plaintiff and the Nationwide Class)

97. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs.

98. As a citizen of Indiana, Anthem is subject to Indiana law in its dealings throughout the United States.

99. Indiana prohibits a person from engaging in deceptive acts, which are specifically defined in relevant part as representations:

> (1) That such subject of a consumer transaction has . . . characteristics . . . it does not have which the supplier knows or should reasonably know it does not have.
>
> (2) That such subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and the supplier knows or should reasonably know that it is not.
>
> (6) That a specific price advantage exists as to such subject of a consumer transaction, if it does not and if the supplier knows or should reasonably know that it does not.

IND. CODE § 24-5-0.5-3(a). A "consumer transaction" includes the sale of personal property for purposes that are primarily personal. IND. CODE § 24-5-0.5-2(1). "Person" includes a corporation. IND. CODE § 24-5-0.5-2(2). "Supplier" is a seller or other person who regularly engages in or solicits consumer transactions and includes a manufacturer "whether or not the person deals directly with the consumer." IND. CODE § 24-5-0.5-2(a)(3).

100. The statute is to be liberally construed and applied to promote its purposes, which are to "(1) simplify, clarify, and modernize the law governing deceptive and unconscionable consumer sales practices; (2) protect consumers from suppliers who commit deceptive and unconscionable sales acts; and (3) encourage the development of fair consumer sales practices." IND. CODE § 24-5-0.5-1(a), (b).

101. For the reasons discussed above, Anthem violated (and, on information and belief, continues to violate) § 24-5-0.5 by engaging in the above-described and prohibited unlawful, unfair, fraudulent, deceptive, untrue, and misleading acts and practices.

102. Anthem violated § 24-5-0.5 by accepting and storing Plaintiff's and the Class members' personal and financial information but failing to take reasonable steps to protect it. In violation of industry standards and best practices, Anthem also violated consumer expectations to safeguard personal and financial information and failed to tell consumers that it did not have reasonable and best practices, safeguards and data security in place.

103. Anthem also violated § 24-5-0.5 by failing to immediately notify Plaintiff and the Class of the Anthem data breach. If Plaintiff and the Class had been notified in an appropriate

fashion, they could have taken precautions to better safeguard their personal and financial information.

104. "A person relying upon an uncured or incurable deceptive act may bring an action for the damages actually suffered as a consumer as a result of the deceptive act or five hundred dollars ($500), whichever is greater." IND. CODE § 24-5-0.5-4(a). An "uncured deceptive act" occurs when a consumer who has been damaged gives pre-suit notice and the defendant fails to cure. IND. CODE § 24-5-0.5-2(a)(7). An "incurable deceptive act" is one "done by a supplier as part of a scheme, artifice, or device with intent to defraud or mislead." IND. CODE § 24-5-0.5-2(a)(8). If the defendant is found to have acted willfully, the Court may treble the damages or award $1,000, whichever is greater. IND. CODE § 24-5-0.5-4(a).

105. On information and belief, Anthem's unlawful, fraudulent, and unfair business acts and practices, except as otherwise indicated herein, continue to this day and are ongoing. As a direct and/or proximate result of Anthem's unlawful, unfair, and fraudulent practices, Plaintiff and the Class have suffered injury in fact and lost money in connection with the Anthem data breach, for which they are entitled to compensation – as well as restitution, disgorgement, and/or other equitable relief. Plaintiff and the Class were injured in fact by: unauthorized activity on their accounts; damage to credit scores and credit reports; time and expense related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards; (c) credit monitoring and identity theft prevention; (d) imposition of withdrawal and purchase limits on compromised accounts; (e) inability to withdraw funds held in linked checking accounts; (f) trips to banks and waiting in line to obtain funds held in limited accounts; (g) resetting automatic billing instructions; (h) late fees and declined payment fees imposed as a result of failed automatic payments; (i) the general nuisance and annoyance of dealing with all these issues resulting from the Anthem data breach; and (j) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the Anthem data breach, all of which have an ascertainable monetary value to be proven at trial.

COUNT VI

Violation of California Data Breach Act

CAL. CIV. CODE § 1798.80, *et seq.*

(On Behalf of Plaintiff and the California Subclass)

106. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs.

107. Section 1798.82 of the CALIFORNIA CIVIL CODE provides, in pertinent part, as follows:

> (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
>
> (b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
>
> (c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
>
> (d) Any person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
>
> > (1) The security breach notification shall be written in plain language.
> >
> > (2) The security breach notification shall include, at a minimum, the following information:

> (A) The name and contact information of the reporting person or business subject to this section.
>
> (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
>
> (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
>
> (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
>
> (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
>
> (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.
>
> * * *
>
> (f) Any person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.
>
> (g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

108. The Anthem data breach constituted a "breach of the security system" of Anthem.

109. Plaintiff's names, addresses, emails, birthdates, Social Security numbers, employment and income information constitute "personal information."

110. Anthem unreasonably delayed in informing anyone about the breach of security of Class members' confidential and non-public information after Anthem knew the data breach had occurred.

111. Anthem failed to disclose to Class members without unreasonable delay and in the most expedient time possible, the breach of security of consumers' personal and financial information when they knew or reasonably believed such information had been compromised.

112. Upon information and belief, no law enforcement agency instructed Anthem that notification to Class members would impede investigation.

113. Pursuant to Section 1798.84 of the CALIFORNIA CIVIL CODE:

> (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.
>
> (b) Any customer injured by a violation of this title may institute a civil action to recover damages.
>
> (c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.
>
> * * *
>
> (e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

114. Plaintiff individually and on behalf of the Class seek all remedies available under CAL. CIV. CODE § 1798.84, including, but not limited to: (a) damages suffered by Class members as alleged above; (b) statutory damages for Anthem's willful, intentional, and/or reckless violation of CAL. CIV. CODE § 1798.83; and (c) equitable relief.

115. Plaintiff on behalf of themselves and the Class also seek reasonable attorneys' fees and costs under CAL. CIV. CODE § 1798.84(g).

COUNT VII

Violation of the California Confidentiality of Medical Information Act

CAL. CIV. CODE § 56, *et seq.*

(On Behalf of Plaintiff and the California Subclass)

116. Plaintiff incorporates the substantive allegations contained in all previous paragraphs as if fully set forth herein.

117. Anthem is a provider of health care within the meaning of Civil Code § 56.06(a) and maintains medical information as defined by Civil Code § 56.05(g).

118. Plaintiff is a patient of Anthem, as defined in Civil Code § 56.05(h). Anthem maintains personal medical information of Plaintiff and the Class.

119. Anthem has misused and/or disclosed medical information regarding Plaintiff without written authorization compliant with the provisions of Civil Code § 56, et seq.

120. Anthems' misuse and/or disclosure of medical information regarding the Plaintiff and the Class constitute a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

121. Plaintiff and the Class have suffered damages from the improper misuse and/or disclosure of their medical information and therefore Plaintiff and the Class seek relief under Civil Code §§ 56.35 and 56.36.

122. Plaintiff and the Class seek actual damages, statutory damage, statutory penalties, attorney fees and costs pursuant to Civil Code §§ 56.35 and 56.36.

COUNT VIII

Violation of California's Unfair Competition Law ("UCL")

CAL. BUS. & PROF. CODE § 17200, *et seq.*

(On Behalf of Plaintiff and the California Subclass)

123. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs.

124. Anthem engaged in unfair, unlawful, and fraudulent business practices in violation of the UCL.

125. California Business & Professions Code § 17200 prohibits any "unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." For the reasons discussed above, Anthem violated (and, on information and belief, continues to violate) California Business & Professions Code § 17200 by engaging in the above-described and prohibited unlawful, unfair, fraudulent, deceptive, untrue, and misleading acts and practices.

126. Anthem violated the UCL by accepting and storing Plaintiff's and the Class members' personal and financial information but failing to take reasonable steps to protect it. In violation of industry standards and best practices, Anthem also violated consumer expectations to safeguard personal and financial information and failed to tell consumers that it did not have reasonable and best practices, safeguards and data security in place.

127. Anthem also violated the UCL by failing to immediately notify Plaintiff and the Class of the Anthem data breach. If Plaintiff and the Class had been notified in an appropriate fashion, they could have taken precautions to better safeguard their personal and financial information.

128. Anthem's above-described wrongful acts and practices also constitute "unlawful" business acts and practices in violation of California's fraud and deceit statutes, CIVIL CODE §§ 1572, 1573, 1709, 1711, California's Data Breach Act, CIVIL CODE § 1798.80, *et seq.*, BUSINESS & PROFESSIONS CODE §§ 17200, *et seq.*, §§ 17500, *et seq.*, and the common law.

129. Anthem's above-described wrongful acts and practices also constitute "unfair" business acts and practices, in that the harm caused by Anthem's above wrongful conduct outweighs any utility of such conduct, and such conduct (i) offends public policy, (ii) is immoral, unscrupulous, unethical, oppressive, deceitful and offensive, and/or (iii) has caused (and will continue to cause) substantial injury to consumers, such as Plaintiff and the Class. There were reasonably available alternatives to further Anthem's legitimate business interests, including using best practices to protect the personal and financial information, other than Anthem's wrongful conduct described herein.

130. Plaintiff alleges violations of California consumer protection and unfair competition laws resulting in harm to consumers. Plaintiff asserts violations of public policy against engaging

in unfair competition, and deceptive conduct towards consumers. This conduct also constitutes violations of the "unfair" prong of California Business and Professions Code § 17200.

131. On information and belief, Anthem's unlawful, fraudulent, and unfair business acts and practices, except as otherwise indicated herein, continue to this day and are ongoing. As a direct and/or proximate result of Anthem's unlawful, unfair, and fraudulent practices, Plaintiff and the Class have suffered injury in fact and lost money in connection with the Anthem data breach, for which they are entitled to compensation – as well as restitution, disgorgement, and/or other equitable relief. Plaintiff and the Class were injured in fact by: fraud on their accounts; damage to credit scores and credit reports; time and expense related to: (a) finding fraudulent charges and accounts; (b) cancelling and reissuing cards; (c) credit monitoring and identity theft prevention; (d) imposition of withdrawal and purchase limits on compromised accounts; (e) trips to banks and waiting in line to obtain funds held in limited accounts; (f) resetting automatic billing instructions; (g) late fees and declined payment fees imposed as a result of failed automatic payments; (h) the general nuisance and annoyance of dealing with all these issues resulting from the Anthem data breach; and (i) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the Anthem data breach, all of which have an ascertainable monetary value to be proven at trial.

132. Plaintiff, for himself and the Class, also are entitled to injunctive relief, under California Business and Professions Code §§ 17203, 17204, to stop Anthem's above-described wrongful acts and practices and require Anthem to maintain adequate or reasonable security measures to protect the personal and financial information in its possession or, in the alternative, for restitution and/or disgorgement.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

A. That the Court certify this case as a class action and appoint the named Plaintiff to be Class representative and his counsel to be Class counsel;

B. That the Court award Plaintiff and the Class appropriate relief, to include actual and statutory damages, disgorgement, and restitution;

C. That the Court award Plaintiff and the Class preliminary or other equitable or declaratory relief as may be appropriate by way of applicable state or federal law;

D. Such additional orders or judgments as may be necessary to prevent these practices and to restore to any person in interest any money or property which may have been acquired by means of the violations; and

E. That the Court award Plaintiff and the Class such other, favorable relief as may be available and appropriate under law or at equity.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all issues so triable.

DATED: February 10, 2015

By */s/ Thomas E. Loeser*
Thomas E. Loeser (202724)

Steve W. Berman (*pro hac vice* pending)
Thomas E. Loeser (SBN 202724)
HAGENS BERMAN SOBOL SHAPIRO LLP
1918 Eighth Avenue, Suite 3300
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594

Mark P. Robinson, Jr. (SBN 054426)
Daniel S. Robinson (SBN 244245)
Wesley K. Polischuk (SBN 254121)
ROBINSON CALCAGNIE ROBINSON SHAPIRO DAVIS, INC.
19 Corporate Plaza Drive
Newport Beach, California 92660
Telephone: (949) 720-1288
Facsimile: (949) 720-1292

Attorneys for Plaintiff and the Proposed Class